(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0044454**

(51)[7] **G06F 21/50**; H04L 29/06; G06F 21/62

(13) **B**

(21) 1-2019-04836
(22) 28/02/2018
(86) PCT/KR2018/002420 28/02/2018
(87) WO/2018/164408 13/09/2018
(30) 10-2017-0028955 07/03/2017 KR
(45) 25/03/2025 444
(43) 30/01/2020 382A
(71) KB FINANCIAL GROUP (KR)
26, Gukjegeumyung-ro 8-gil, Yeongdeungpo-gu, Seoul 07331, Republic of Korea
(72) PARK, Hyoung Joo (KR); KIM, Young Kyun (KR); PARK, Chun Il (KR); KIM, Yang Ho (KR); KIM, Ki Woong (KP).
(74) CÔNG TY TRÁCH NHIỆM HỮU HẠN TƯ VẤN ĐẦU TƯ VÀ SỞ HỮU TRÍ TUỆ INTERFIVE (INTERFIVE CO., LTD)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP GIỮ AN TOÀN CHO ỨNG DỤNG

(21) 1-2019-04836

(57) Sáng chế đề cập đến hệ thống và phương pháp giữ an toàn cho ứng dụng. Hệ thống giữ an toàn cho ứng dụng theo một phương án làm ví dụ thực hiện sáng chế bao gồm: thiết bị máy khách, để tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động, truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn, và truyền yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động theo thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra; máy chủ kiểm tra, để thu nhận yêu cầu kiểm tra từ thiết bị máy khách, kiểm tra ứng dụng thiếu an toàn, và truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách; và máy chủ quản lý, để thu nhận yêu cầu tệp an toàn từ thiết bị máy khách và truyền tệp liên quan đến độ an toàn động đã được mã hoá đến thiết bị máy khách.

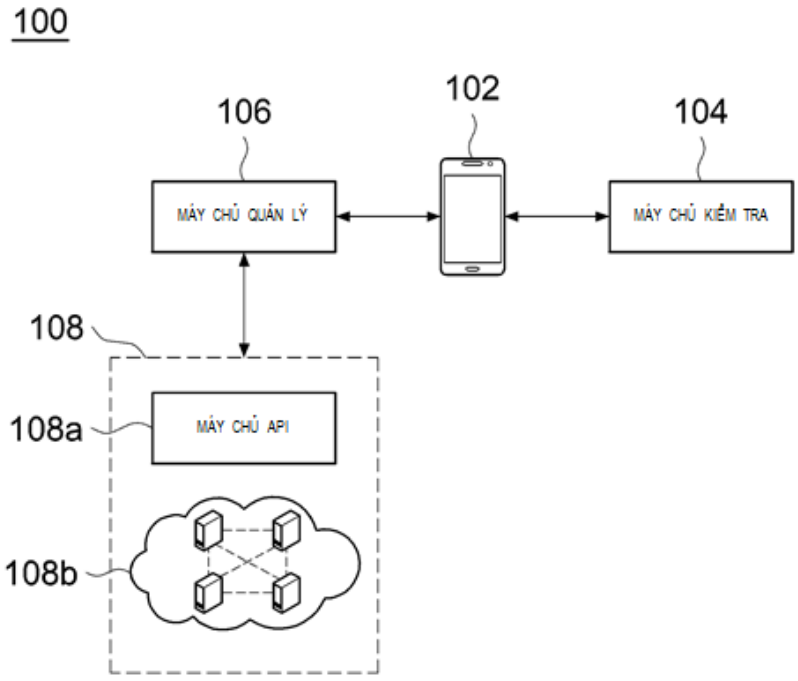


FIG.1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến kỹ thuật an toàn.

Tình trạng kỹ thuật của sáng chế

Do việc sử dụng máy điện thoại thông minh tăng vọt trong những năm gần đây, nên các trường hợp ứng dụng sử dụng các ứng dụng được cài đặt trên máy điện thoại thông minh cũng tăng lên. Ví dụ, số lượng trường hợp thực hiện giao dịch tài chính hoặc thanh toán bằng cách sử dụng ứng dụng được cài đặt trên máy điện thoại thông minh ngày càng tăng lên. Tuy nhiên, có vấn đề phát sinh là ứng dụng để thực hiện các giao dịch tài chính hoặc thanh toán có thể bị xâm nhập trái phép hoặc đánh cắp bởi bên thứ ba với mục đích bất hợp pháp.

Bản chất kỹ thuật của sáng chế

Các phương án làm ví dụ thực hiện sáng chế nhằm mục đích đề xuất phương pháp giữ an toàn cho ứng dụng có khả năng nâng cao độ an toàn khi sử dụng ứng dụng và hệ thống để thực hiện phương pháp giữ an toàn cho ứng dụng này.

Theo một khía cạnh của sáng chế, sáng chế đề xuất hệ thống giữ an toàn cho ứng dụng bao gồm: thiết bị máy khách được tạo cấu hình để tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động, truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn, và truyền yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động theo thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra; máy chủ kiểm tra được tạo cấu hình để thu nhận yêu cầu kiểm tra từ thiết bị máy khách và truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách; và máy chủ quản lý được tạo cấu hình để thu nhận yêu cầu tệp an toàn từ thiết bị máy khách và truyền tệp liên quan đến độ an toàn động đã được mã hoá đến thiết bị máy khách.

Yêu cầu kiểm tra có thể chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách.

Máy chủ kiểm tra có thể thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng

đã được lưu trữ từ trước của ứng dụng thiếu an toàn, tạo ra giá trị khoá mã hoá dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách theo kết quả kiểm tra, và truyền thông tin liên quan đến kết quả kiểm tra chứa kết quả kiểm tra và giá trị khoá mã hoá đến thiết bị máy khách.

Khi có hiện tượng bất thường xảy ra, máy chủ kiểm tra có thể tạo ra giá trị khoá mã hoá dựa vào thông tin duy nhất để quản lý trong đó kết hợp thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin quản lý giả định trước.

Khi tổng số lần kiểm tra không thành công theo yêu cầu kiểm tra của mỗi thiết bị máy khách trong một khoảng thời gian định trước vượt quá số lần thứ nhất định trước, thì máy chủ kiểm tra có thể xác định rằng có hiện tượng bất thường xảy ra.

Khi tổng số lần kiểm tra không thành công theo yêu cầu kiểm tra của thiết bị máy khách vượt quá số lần thứ hai định trước, thì máy chủ kiểm tra có thể xác định rằng có hiện tượng bất thường xảy ra.

Yêu cầu tệp an toàn có thể chứa thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

Máy chủ quản lý có thể tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách, mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá, và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách.

Yêu cầu tệp an toàn có thể chứa ít nhất một thông tin trong số thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

Hệ thống giữ an toàn cho ứng dụng này có thể còn bao gồm chuỗi khối được tạo cấu hình để thu nhận thông tin nhận dạng duy nhất của mỗi thiết bị máy khách và giá trị khoá mã hoá từ máy chủ quản lý và so khớp và lưu trữ thông tin nhận dạng duy nhất của mỗi thiết bị máy khách và giá trị khoá mã hoá tương ứng.

Máy chủ quản lý có thể truyền thông tin nhận dạng duy nhất của thiết bị máy khách

có trong yêu cầu tệp an toàn đến chuỗi khối, chuỗi khối có thể tách ra giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách và truyền giá trị khoá mã hoá đã tách ra đến máy chủ quản lý, và máy chủ quản lý có thể tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách, mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được từ chuỗi khối, và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách.

Thiết bị máy khách có thể giải mã tệp liên quan đến độ an toàn động đã được mã hoá dựa vào giá trị khoá mã hoá và tệp liên quan đến độ an toàn động có thể chứa lệnh để nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ của thiết bị máy khách theo dung lượng còn lại của bộ nhớ.

Tệp liên quan đến độ an toàn tĩnh có thể chứa lệnh để truyền yêu cầu kiểm tra đến máy chủ kiểm tra ở thời điểm thực hiện ứng dụng thiếu an toàn và lệnh để kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra theo thông tin liên quan đến kết quả kiểm tra chỉ báo rằng việc kiểm tra ứng dụng thiếu an toàn không thành công.

Theo một khía cạnh khác của sáng chế, sáng chế đề xuất phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy khách có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước: tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động; truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn; thu nhận thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra và truyền yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động theo thông tin liên quan đến kết quả kiểm tra; thu nhận tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá tương ứng với yêu cầu tệp an toàn; và giải mã tệp liên quan đến độ an toàn động đã được mã hoá bằng cách sử dụng giá trị khoá mã hoá.

Yêu cầu kiểm tra có thể chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách.

Thông tin liên quan đến kết quả kiểm tra có thể chứa kết quả kiểm tra thu được sau

khi thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn và giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách.

Yêu cầu tệp an toàn có thể chứa thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

Tệp liên quan đến độ an toàn động có thể chứa lệnh để kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách, lệnh để so sánh dung lượng còn lại của bộ nhớ và dung lượng của tệp liên quan đến độ an toàn động, và lệnh để nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ theo kết quả so sánh.

Tệp liên quan đến độ an toàn động có thể chứa lệnh để truyền yêu cầu kiểm tra ở thời điểm thực hiện ứng dụng thiếu an toàn và lệnh để kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra theo thông tin liên quan đến kết quả kiểm tra chỉ báo rằng việc kiểm tra ứng dụng thiếu an toàn không thành công.

Theo một khía cạnh khác nữa của sáng chế, sáng chế đề xuất phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy tính có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước: thu nhận, từ thiết bị máy khách, yêu cầu kiểm tra đối với một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động; thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn; và tạo ra thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra và truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách, trong đó yêu cầu kiểm tra chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách và bước tạo ra thông tin liên quan đến kết quả kiểm tra bao gồm bước tạo ra giá trị khoá mã hoá dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách theo kết quả kiểm tra.

Bước tạo ra giá trị khoá mã hoá có thể bao gồm bước tạo ra giá trị khoá mã hoá

bằng cách băm thông tin nhận dạng duy nhất của thiết bị máy khách khi kết quả kiểm tra chỉ báo việc kiểm tra thành công.

Bước tạo ra giá trị khoá mã hoá có thể bao gồm bước xác định xem hiện tượng bất thường có xảy ra hay không dựa vào thông tin nhật ký theo yêu cầu kiểm tra của mỗi thiết bị máy khách, và khi có hiện tượng bất thường xảy ra, tạo ra giá trị khoá mã hoá dựa vào thông tin duy nhất để quản lý trong đó kết hợp thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin quản lý giả định trước.

Theo một khía cạnh khác nữa của sáng chế, sáng chế đề xuất phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy tính có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước: thu nhận, từ thiết bị máy khách để tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động, yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động; tách ra thông tin nhận dạng duy nhất của thiết bị máy khách có trong yêu cầu tệp an toàn; truyền thông tin nhận dạng duy nhất đã tách ra của thiết bị máy khách đến chuỗi khối; thu nhận, từ chuỗi khối, giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách; và mã hoá tệp liên quan đến độ an toàn động bằng cách sử dụng giá trị khoá mã hoá thu được và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách.

Yêu cầu tệp an toàn có thể chứa thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin liên quan đến hệ điều hành của thiết bị máy khách và bước truyền tệp liên quan đến độ an toàn động đã được mã hoá có thể bao gồm bước tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách và mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được.

Theo các phương án thực hiện sáng chế, ứng dụng thiếu an toàn được phân phối cho thiết bị máy khách và tệp liên quan đến độ an toàn đã được mã hoá được truyền mỗi khi ứng dụng thiếu an toàn này được thực hiện, cho nên có thể giảm đến mức thấp nhất sự bộc lộ phần thông tin an toàn của ứng dụng đã được nạp vào thiết bị máy khách và có thể

ngăn chặn không để cho tệp liên quan đến độ an toàn của ứng dụng tương ứng bị xâm nhập trái phép hoặc đánh cắp bởi bên thứ ba có ác ý.

Ngoài ra, máy chủ kiểm tra thực hiện quy trình kiểm tra ứng dụng thiếu an toàn và do đó truyền giá trị khoá mã hoá đến thiết bị máy khách, cho nên có thể xác nhận tính nguyên vẹn để biết ứng dụng tương ứng có bị giả mạo hoặc can thiệp hay không. Đồng thời, giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách, cho nên có thể cho phép quy trình mã hoá và giải mã được thực hiện khác nhau đối với mỗi thiết bị máy khách, nhờ đó nâng cao độ an toàn khi sử dụng ứng dụng.

Hơn nữa, ứng dụng thiếu an toàn được phân phối cho thiết bị máy khách, cho nên kích thước của ứng dụng được phân phối cho thiết bị máy khách có thể được giảm đến mức thấp nhất, và ngay cả khi tệp liên quan đến độ an toàn động được sửa đổi hoặc cập nhật, ứng dụng này không cần phải được tải xuống lại và có thể tự động thu nhận và thực hiện tệp liên quan đến độ an toàn động đã được cập nhật ở thời điểm thực hiện ứng dụng.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ thể hiện cấu hình của hệ thống giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế.

Fig.2 là lưu đồ thể hiện quy trình kiểm tra sự giả mạo/can thiệp trong phương pháp giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế.

Fig.3 là lưu đồ thể hiện quy trình thu nhận tệp liên quan đến độ an toàn động trong phương pháp giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế.

Fig.4 là sơ đồ khối để mô tả môi trường thiết bị máy tính 10 có thiết bị máy tính phù hợp được sử dụng trong các phương án làm ví dụ thực hiện sáng chế.

Mô tả chi tiết sáng chế

Phần mô tả sáng chế dưới đây được nêu ra để giúp cho người đọc hiểu hoàn toàn về các phương pháp, các thiết bị, và/hoặc các hệ thống được mô tả trong sáng chế. Do đó, nhiều phương án thay đổi, phương án cải biến, và phương án tương đương của các phương pháp, các thiết bị, và/hoặc các hệ thống được mô tả trong sáng chế sẽ được tìm ra đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật này.

Các chức năng và các cấu trúc đã biết có thể không được mô tả trong sáng chế để làm cho bản mô tả sáng chế rõ ràng và ngắn gọn hơn. Đồng thời, các thuật ngữ được sử dụng dưới đây được lựa chọn bằng cách xem xét các chức năng theo phương án thực hiện sáng chế và nghĩa của các thuật ngữ này có thể thay đổi tuỳ theo, ví dụ, ý định hoặc thói quen của người dùng hoặc người vận hành. Vì vậy, định nghĩa của các thuật ngữ này sẽ được xác định dựa vào ngữ cảnh chung. Thuật ngữ được dùng trong phần mô tả chi tiết sáng chế được sử dụng chỉ nhằm mục đích mô tả các phương án thực hiện sáng chế và không nhằm mục đích giới hạn phạm vi của sáng chế. Một danh từ chung khi được dùng trong sáng chế được hiểu theo nghĩa là danh từ đó dùng ở dạng số ít cũng như danh từ đó dùng ở dạng số nhiều, trừ trường hợp danh từ đó có định nghĩa khác một cách rõ ràng theo ngữ cảnh. Cần phải hiểu rằng các chữ "bao gồm" hoặc "có" xác định rõ một số đặc trưng, trị số, bước, thao tác, bộ phận, và/hoặc các dạng kết hợp của các loại nêu trên khi được dùng trong sáng chế, nhưng không loại trừ sự có mặt hoặc khả năng xuất hiện thêm của một hoặc nhiều đặc trưng, trị số, bước, thao tác, bộ phận khác, và/hoặc các dạng kết hợp khác của các loại nêu trên trong sáng chế.

Trong phần mô tả sáng chế dưới đây, các thuật ngữ "chuyển", "truyền thông", "truyền", "thu", hoặc các thuật ngữ tương tự khác biểu thị rằng tín hiệu hoặc thông tin được truyền từ bộ phận này đến bộ phận khác một cách trực tiếp hoặc thông qua các bộ phận trung gian. Cụ thể là, khi sáng chế mô tả rằng tín hiệu hoặc thông tin được "chuyển" hoặc "truyền" đến một bộ phận, thì điều này có nghĩa là bộ phận đó là đích đến cuối cùng chứ không phải là đích đến trực tiếp. Điều này cũng có thể được áp dụng cho trường hợp trong đó tín hiệu hoặc thông tin được "thu". Trong phần mô tả sáng chế, khi sáng chế mô tả rằng hai dữ liệu hoặc thông tin có "liên hệ" với nhau, thì điều này có nghĩa là, nếu thu được một dữ liệu (hoặc thông tin), thì có thể thu được ít nhất là các dữ liệu (hoặc thông tin) còn lại dựa vào sự liên hệ đó.

Fig.1 là sơ đồ thể hiện cấu hình của hệ thống giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế.

Dựa vào Fig.1, hệ thống giữ an toàn cho ứng dụng 100 có thể bao gồm thiết bị máy khách 102, máy chủ kiểm tra 104, máy chủ quản lý 106, và chuỗi khối 108. Trong đó, thiết bị máy khách 102 được kết nối truyền thông với mỗi máy chủ trong số máy chủ

kiểm tra 104 và máy chủ quản lý 106 qua mạng truyền thông. Ngoài ra, máy chủ quản lý 106 được kết nối truyền thông với chuỗi khối 108 qua mạng truyền thông. Theo một số phương án thực hiện sáng chế, mạng truyền thông có thể là mạng internet, một hoặc nhiều mạng cục bộ (Local Area Network, LAN), mạng diện rộng, mạng truyền thông chia ô, mạng truyền thông di động, và các mạng khác, hoặc các dạng kết hợp của các loại mạng nêu trên.

Thiết bị máy khách 102 là thiết bị truyền thông mà người dùng sử dụng. Ví dụ về thiết bị máy khách 102 là các thiết bị truyền thông nối dây/không dây thuộc nhiều loại khác nhau, như máy điện thoại di động, máy điện thoại thông minh, thiết bị dạng bảng, thiết bị đeo được, máy tính xách tay, và các thiết bị khác, các thiết bị này có thể truy nhập vào các thiết bị máy chủ 104 và 106.

Người dùng sử dụng thiết bị máy khách 102 có thể tải xuống một ứng dụng định trước từ thiết bị máy chủ (ví dụ, máy chủ kiểm tra 104, máy chủ quản lý 106, hoặc thiết bị máy chủ khác không được thể hiện trên Fig.1). Ứng dụng đã tải xuống có thể được lưu trữ vào vật ghi đọc được bằng máy tính của thiết bị máy khách 102. Ứng dụng này có thể chứa một tập hợp gồm các lệnh định trước có thể thực hiện được bằng bộ xử lý của thiết bị máy khách 102. Các lệnh trong ứng dụng có thể được tạo cấu hình để, khi được thực hiện bằng bộ xử lý của thiết bị máy khách 102, ra lệnh cho bộ xử lý thực hiện các thao tác theo phương án làm ví dụ thực hiện sáng chế. Vật ghi đọc được bằng máy tính có các thành phần của hệ điều hành để thực hiện một tập hợp lệnh, như ứng dụng, trên thiết bị máy khách 102. Ví dụ, hệ điều hành có thể là iOS của Apple Inc. hoặc Android của Google.

Ứng dụng được tải xuống bằng thiết bị máy khách 102 có thể là ứng dụng để thực hiện nhiệm vụ cần có độ an toàn, như các giao dịch tài chính trực tuyến (chuyển khoản, thanh toán, v.v.). Ví dụ, ứng dụng đã tải xuống có thể là ứng dụng giao dịch ngân hàng qua mạng internet. Tuy nhiên, một phần trong số các tệp liên quan đến độ an toàn có thể bị thiếu (tức là, chỉ có một phần trong số các tệp liên quan đến độ an toàn) trong ứng dụng được tải xuống. Có nghĩa là, ứng dụng được tải xuống là để thực hiện trực tuyến nhiệm vụ cần có độ an toàn, nhưng ứng dụng này có thể đang ở trạng thái mà ở đó nó không thể thực hiện được một cách bình thường hoặc hoàn toàn nhiệm vụ cần có độ an

toàn đó vì một phần trong số các tệp liên quan đến độ an toàn bị thiếu. Dưới đây, ứng dụng được tải xuống có thể được gọi là một ứng dụng thiếu an toàn.

Theo phương án làm ví dụ thực hiện sáng chế, các tệp liên quan đến độ an toàn có thể gồm có tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động. Ứng dụng thiếu an toàn có thể là ứng dụng mà trên đó chỉ được nạp tệp liên quan đến độ an toàn tĩnh, trong số các tệp liên quan đến độ an toàn, và không được nạp tệp liên quan đến độ an toàn động. Trong đó, tệp liên quan đến độ an toàn tĩnh có thể là tệp có độ an toàn cơ bản của ứng dụng thiếu an toàn. Tệp liên quan đến độ an toàn tĩnh có thể được sử dụng để thực hiện, ví dụ, chức năng xác thực người dùng, điều khiển truy nhập, chống gỡ rối, bảo vệ mã nguồn, và các chức năng khác. Chức năng xác thực người dùng có thể được hiểu là chức năng thực hiện quy trình xác thực người dùng dựa vào từ khoá, xác thực thông tin sinh trắc, chứng chỉ công cộng, số pin, và các thông tin khác ở thời điểm thực hiện ứng dụng thiếu an toàn. Chức năng điều khiển truy nhập có thể được hiểu là chức năng kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra đối với yêu cầu kiểm tra, như sẽ được mô tả dưới đây, chỉ báo rằng việc kiểm tra không thành công. Tệp liên quan đến độ an toàn động có thể là tệp có độ an toàn bổ sung của ứng dụng thiếu an toàn. Tệp liên quan đến độ an toàn động có thể có chức năng, ví dụ, bảo mật bàn phím, phát hiện sự can thiệp vào phần gốc, chương trình phòng ngừa virut, và các chức năng khác. Theo một phương án thực hiện sáng chế, tệp liên quan đến độ an toàn tĩnh có thể là tệp liên quan đến độ an toàn được nạp trên ứng dụng thiếu an toàn và tệp liên quan đến độ an toàn động có thể là tệp liên quan đến độ an toàn không được nạp trên ứng dụng thiếu an toàn và sẽ được thu nhận riêng biệt từ nguồn bên ngoài.

Như đã được mô tả trên đây, thiết bị máy khách 102 tải xuống ứng dụng trong đó một phần trong số các tệp liên quan đến độ an toàn bị thiếu (tức là, tệp liên quan đến độ an toàn động bị thiếu), và do đó cần phải thu nhận tệp liên quan đến độ an toàn động từ nguồn bên ngoài khi ứng dụng thiếu an toàn được thực hiện.

Cụ thể là, thiết bị máy khách 102 có thể truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn đến máy chủ kiểm tra 104 khi người dùng thực hiện ứng dụng thiếu an toàn. Yêu cầu kiểm tra có thể chứa thông tin nhận dạng (ví dụ, thông tin nhận dạng (Identification information, ID) của ứng dụng thiếu an toàn, giá trị băm của ứng dụng

thiếu an toàn, và các thông tin khác) của ứng dụng thiếu an toàn. Ngoài ra, yêu cầu kiểm tra có thể còn chứa thông tin duy nhất để quản lý được sử dụng để tạo ra giá trị khoá mã hoá duy nhất cho thiết bị máy khách tương ứng 102. Theo phương án làm ví dụ thực hiện sáng chế, thông tin duy nhất để quản lý có thể là thông tin nhận dạng duy nhất của thiết bị máy khách tương ứng 102.

Trong trường hợp này, thông tin nhận dạng duy nhất của thiết bị máy khách 102 có thể thay đổi theo hệ điều hành của thiết bị máy khách 102. Ví dụ, khi hệ điều hành của thiết bị máy khách 102 là Android, thì thông tin nhận dạng duy nhất có thể là thông tin nhận dạng duy nhất toàn cầu (Universally Unique Identifier, UUID), thông tin nhận dạng thiết bị di động quốc tế (International Mobile Equipment Identifier, IMEI), số thứ tự của thẻ môđun nhận dạng thuê bao (Subscriber Identification Module, SIM), giá trị duy nhất nhận dạng thiết bị của thiết bị máy khách 102. Ví dụ khác, thông tin nhận dạng duy nhất của thiết bị máy khách 102 có thể là giá trị duy nhất nhận dạng thiết bị của thiết bị máy khách 102. Thông tin nhận dạng duy nhất của thiết bị máy khách 102 có thể được đưa vào trong yêu cầu kiểm tra được truyền lần đầu tiên.

Thiết bị máy khách 102 có thể thu nhận thông tin liên quan đến kết quả kiểm tra đối với yêu cầu kiểm tra từ máy chủ kiểm tra 104. Thông tin liên quan đến kết quả kiểm tra có thể chứa kết quả kiểm tra đối với yêu cầu kiểm tra, thời gian kiểm tra, và giá trị khoá mã hoá. Trong đó, giá trị khoá mã hoá có thể là giá trị (tức là, giá trị băm) thu được bằng cách băm thông tin nhận dạng duy nhất của thiết bị máy khách 102. Giá trị khoá mã hoá có thể được đưa vào thông tin liên quan đến kết quả kiểm tra chỉ khi kết quả kiểm tra chỉ báo việc kiểm tra thành công.

Thiết bị máy khách 102 có thể kiểm tra thông tin liên quan đến kết quả kiểm tra, và khi kết quả kiểm tra chỉ báo rằng việc kiểm tra không thành công, có thể kết thúc ứng dụng thiếu an toàn. Trong trường hợp này, thiết bị máy khách 102 có thể thông báo cho người dùng biết rằng ứng dụng thiếu an toàn đã kết thúc. Thiết bị máy khách 102 có thể thực hiện thao tác này dựa vào tệp liên quan đến độ an toàn tĩnh có trong ứng dụng thiếu an toàn. Có nghĩa là, tệp liên quan đến độ an toàn tĩnh có thể chứa lệnh được dùng để kết thúc ứng dụng thiếu an toàn trong trường hợp kiểm tra không thành công.

Như đã được mô tả trên đây, quy trình kiểm tra ứng dụng thiếu an toàn được thực

hiện, và khi việc kiểm tra không thành công, thì ứng dụng thiếu an toàn sẽ được kết thúc, nhờ đó bảo đảm sơ bộ sự an toàn (tức là, độ an toàn) của ứng dụng. Nói cách khác, bằng cách thực hiện ứng dụng sau khi kiểm tra xem ứng dụng có bị giả mạo hoặc can thiệp hay không, có thể xác nhận tính nguyên vẹn của ứng dụng đã tải xuống.

Tuy nhiên, khi kết quả kiểm tra thu được chỉ báo việc kiểm tra thành công, thì thiết bị máy khách 102 có thể truyền yêu cầu tệp an toàn đến máy chủ quản lý 106. Trong đó, yêu cầu tệp an toàn có thể chứa thông tin nhận dạng duy nhất và giá trị khoá mã hoá của thiết bị máy khách 102. Có nghĩa là, thiết bị máy khách 102 có thể có, ở trong yêu cầu tệp an toàn, giá trị khoá mã hoá thu được từ máy chủ kiểm tra 104 khi truyền yêu cầu tệp an toàn đến máy chủ quản lý 106. Thiết bị máy khách 102 có thể xoá giá trị khoá mã hoá sau khi truyền giá trị khoá mã hoá này đến máy chủ quản lý 106. Trong đó, giá trị khoá mã hoá có thể được đưa vào trong yêu cầu tệp an toàn khi yêu cầu tệp an toàn được truyền lần đầu tiên. Ngoài ra, thông tin liên quan đến hệ điều hành của thiết bị máy khách 102 có thể còn được đưa vào trong yêu cầu tệp an toàn. Trong đó, thông tin liên quan đến hệ điều hành có thể chứa thông tin về loại hệ điều hành và thông tin về phiên bản hệ điều hành.

Thiết bị máy khách 102 có thể thu nhận tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá từ máy chủ quản lý 106. Thiết bị máy khách 102 có thể giải mã tệp liên quan đến độ an toàn động đã được mã hoá bằng cách sử dụng giá trị khoá mã hoá, nạp tệp liên quan đến độ an toàn động đã được giải mã, và sau đó thực hiện tệp liên quan đến độ an toàn động. Sau khi thực hiện tệp liên quan đến độ an toàn động, thiết bị máy khách 102 có thể xoá tệp liên quan đến độ an toàn động. Trong đó, tệp liên quan đến độ an toàn động được xoá ở trạng thái đang được nạp vào vật ghi đọc được bằng máy tính (tức là, bộ nhớ), và do đó tệp liên quan đến độ an toàn động về cơ bản có thể được ngăn chặn không bị biên dịch ngược. Trong trường hợp này, trừ khi bản thân bộ nhớ của thiết bị máy khách 102 bị xâm nhập trái phép, tệp liên quan đến độ an toàn động sẽ không bị rò rỉ cho bên thứ ba.

Tuy nhiên, tệp liên quan đến độ an toàn động có thể chứa các lệnh để kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách 102 và chỉ nạp một số tệp trong số các tệp liên quan đến độ an toàn động vào bộ nhớ khi dung lượng còn lại của bộ nhớ không

đủ để nạp tệp liên quan đến độ an toàn động. Trong số các tệp liên quan đến độ an toàn động, một số tệp trong số các tệp liên quan đến độ an toàn động có thể được nạp vào bộ nhớ theo thứ tự ưu tiên định trước dựa vào dung lượng còn lại của bộ nhớ. Ví dụ, khi các tệp liên quan đến độ an toàn động là chương trình phòng ngừa virut, chương trình bàn phím ảo, và các chương trình khác, thì chương trình phòng ngừa virut, phải sử dụng thường xuyên, so với chương trình bàn phím ảo chỉ được sử dụng khi nhập phím, có thể được ưu tiên nạp vào bộ nhớ.

Thiết bị máy khách 102 có thể thu nhận giá trị khoá mã hoá trong khi kiểm tra ứng dụng tương ứng trên máy chủ kiểm tra 104 ở thời điểm thực hiện ứng dụng thiếu an toàn lần đầu tiên, và có thể truyền yêu cầu tệp an toàn đến máy chủ quản lý 106 để đăng ký thông tin nhận dạng duy nhất của thiết bị máy khách 102 và giá trị khoá mã hoá. Ngoài ra, thiết bị máy khách 102 có thể thu nhận tệp liên quan đến độ an toàn động đã được mã hoá và khoá giải mã từ máy chủ quản lý 106 và giải mã tệp liên quan đến độ an toàn động đã được mã hoá bằng cách sử dụng khoá giải mã. Sau đó, mỗi khi thiết bị máy khách 102 thực hiện ứng dụng thiếu an toàn để thực hiện giao dịch tài chính hoặc thanh toán trực tuyến, thiết bị máy khách 102 có thể thực hiện quy trình kiểm tra trên máy chủ kiểm tra 104 và truyền yêu cầu tệp an toàn động đến máy chủ quản lý 106. Sau đó, máy chủ quản lý 106 mã hoá tệp liên quan đến độ an toàn động bằng cách tách ra giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 có trong yêu cầu tệp an toàn và truyền tệp liên quan đến độ an toàn động đã được mã hoá và khoá mã hoá đến thiết bị máy khách 102.

Máy chủ kiểm tra 104 có thể dùng để kiểm tra ứng dụng thiếu an toàn được phân phối cho mỗi thiết bị máy khách 102. Cụ thể là, máy chủ kiểm tra 104 có thể xác định xem ứng dụng thiếu an toàn có bị giả mạo hoặc can thiệp hay không. Máy chủ kiểm tra 104 có thể lưu trữ thông tin nhận dạng của ứng dụng thiếu an toàn (ví dụ, thông tin ID của ứng dụng thiếu an toàn, giá trị băm của ứng dụng thiếu an toàn, và các thông tin khác) trước khi ứng dụng thiếu an toàn của một phiên bản cụ thể được phân phối.

Máy chủ kiểm tra 104 có thể thu nhận yêu cầu kiểm tra từ mỗi thiết bị máy khách 102 đã thực hiện ứng dụng thiếu an toàn. Máy chủ kiểm tra 104 có thể thực hiện quy trình kiểm tra bằng cách kiểm tra xem thông tin nhận dạng của ứng dụng thiếu an toàn có

trong yêu cầu kiểm tra có trùng khớp với thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn hay không.

Cụ thể là, máy chủ kiểm tra 104 có thể xác định rằng việc kiểm tra thành công (tức là, xác định rằng ứng dụng thiếu an toàn đang xem xét không bị giả mạo hoặc can thiệp) khi thông tin nhận dạng của ứng dụng thiếu an toàn (ví dụ, thông tin ID của ứng dụng thiếu an toàn và giá trị băm của ứng dụng thiếu an toàn) có trong yêu cầu kiểm tra trùng khớp với thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn. Máy chủ kiểm tra 104 có thể xác định rằng việc kiểm tra không thành công (tức là, xác định rằng ứng dụng thiếu an toàn đang xem xét bị giả mạo hoặc can thiệp) khi thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra không trùng khớp với thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn.

Máy chủ kiểm tra 104 có thể tạo ra thông tin liên quan đến kết quả kiểm tra đáp lại yêu cầu kiểm tra của thiết bị máy khách 102 và truyền thông tin liên quan đến kết quả kiểm tra đã tạo ra đến thiết bị máy khách 102. Thông tin liên quan đến kết quả kiểm tra có thể chứa kết quả kiểm tra (tức là, kiểm tra thành công hoặc kiểm tra không thành công) đối với yêu cầu kiểm tra, thời gian kiểm tra, giá trị khoá mã hoá, và các thông tin khác.

Khi thông tin duy nhất để quản lý (ví dụ, thông tin nhận dạng duy nhất của thiết bị máy khách 102) được đưa vào trong yêu cầu kiểm tra, thì máy chủ kiểm tra 104 có thể băm thông tin nhận dạng duy nhất của thiết bị máy khách 102 và sau đó thiết lập giá trị băm của thông tin nhận dạng duy nhất của thiết bị máy khách 102 để làm giá trị khoá mã hoá. Trong đó, giá trị khoá mã hoá có thể là giá trị khoá mã hoá để mã hoá tệp liên quan đến độ an toàn trong máy chủ quản lý 106 và giá trị khoá giải mã để giải mã tệp liên quan đến độ an toàn đã được mã hoá trong thiết bị máy khách 102. Trong trường hợp này, giá trị khoá mã hoá và giá trị khoá giải mã có thể là giống nhau. Máy chủ kiểm tra 104 có thể truyền giá trị khoá mã hoá bằng cách đưa giá trị khoá mã hoá này vào trong thông tin liên quan đến kết quả kiểm tra chỉ khi kết quả kiểm tra chỉ báo việc kiểm tra thành công.

Tuy nhiên, khi xác định rằng có hiện tượng bất thường xảy ra, máy chủ kiểm tra 104 có thể băm thông tin duy nhất để quản lý mà trong đó thông tin quản lý giả định trước được bổ sung vào thông tin nhận dạng duy nhất của thiết bị máy khách 102, và có thể thiết lập giá trị băm để làm giá trị khoá mã hoá. Trong trường hợp này, thông tin duy

nhất để quản lý có thể được tạo ra bằng cách bổ sung thông tin quản lý giả vào phần đầu hoặc phần cuối của thông tin nhận dạng duy nhất của thiết bị máy khách 102.

Có nghĩa là, máy chủ kiểm tra 104 có thể thường tạo ra khoá mã hoá bằng cách thiết lập thông tin nhận dạng duy nhất của thiết bị máy khách 102 để làm thông tin duy nhất để quản lý và, khi xác định rằng có hiện tượng bất thường xảy ra, thì có thể tạo ra khoá mã hoá bằng cách sử dụng thông tin duy nhất để quản lý trong đó kết hợp thông tin nhận dạng duy nhất của thiết bị máy khách 102 và thông tin quản lý giả định trước.

Máy chủ kiểm tra 104 có thể quản lý thông tin nhật ký riêng của thiết bị máy khách theo yêu cầu kiểm tra của mỗi thiết bị máy khách 102. Thông tin nhật ký có thể chứa thời gian thu nhận yêu cầu kiểm tra, kết quả kiểm tra, thời gian truyền thông tin liên quan đến kết quả kiểm tra, và các thông tin khác. Máy chủ kiểm tra 104 có thể xác định xem có hiện tượng bất thường xảy ra hay không, dựa vào thông tin nhật ký theo yêu cầu kiểm tra. Ví dụ, máy chủ kiểm tra 104 có thể xác định rằng có hiện tượng bất thường xảy ra khi tổng số lần kiểm tra không thành công theo yêu cầu kiểm tra của mỗi thiết bị máy khách trong một khoảng thời gian định trước vượt quá số lần thứ nhất định trước. Ngoài ra, máy chủ kiểm tra 104 có thể xác định rằng có hiện tượng bất thường xảy ra khi số lần kiểm tra không thành công theo yêu cầu kiểm tra của thiết bị máy khách định trước 102 vượt quá số lần thứ hai định trước. Trong đó, số lần thứ nhất và số lần thứ hai có thể được thiết lập một cách phù hợp có tính đến số lượng thuê bao dịch vụ và các yếu tố khác.

Như đã được mô tả trên đây, bằng cách thay đổi quy tắc tạo ra giá trị khoá mã hoá trong trường hợp có hiện tượng bất thường xảy ra, có thể ngăn chặn không để cho giá trị khoá mã hoá bị rò rỉ cho bên thứ ba có ác ý.

Máy chủ quản lý 106 có thể thu nhận yêu cầu tệp an toàn từ thiết bị máy khách 102. Máy chủ quản lý 106 có thể xác định xem thiết bị máy khách 102 đã truyền yêu cầu tệp an toàn có phải là thiết bị đã đăng ký hay không, và khi thiết bị máy khách 102 là thiết bị chưa đăng ký, thì có thể đăng ký thiết bị máy khách 102 trong chuỗi khối 108. Cụ thể là, máy chủ quản lý 106 có thể tách ra thông tin nhận dạng duy nhất của thiết bị máy khách 102 từ yêu cầu tệp an toàn và hỏi xem thiết bị máy khách 102 đã được đăng ký hay chưa bằng cách truyền thông tin nhận dạng duy nhất đã tách ra của thiết bị máy khách 102 đến chuỗi khối 108. Khi thiết bị máy khách 102 đang xem xét chưa được đăng ký, thì máy

chủ quản lý 106 có thể truyền giá trị khoá mã hoá có trong yêu cầu tệp an toàn đến chuỗi khối 108 để cho phép thiết bị máy khách 102 được đăng ký. Trong trường hợp này, chuỗi khối 108 có thể đăng ký thông tin nhận dạng duy nhất của thiết bị máy khách 102 bằng cách so khớp thông tin nhận dạng duy nhất và giá trị khoá mã hoá.

Ngoài ra, máy chủ quản lý 106 có thể truyền tệp liên quan đến độ an toàn động đến thiết bị máy khách 102 dựa vào thông tin liên quan đến hệ điều hành của thiết bị máy khách 102 có trong yêu cầu tệp an toàn. Máy chủ quản lý 106 có thể lưu trữ các tệp liên quan đến độ an toàn động theo phiên bản hệ điều hành đối với mỗi loại hệ điều hành. Máy chủ quản lý 106 có thể tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách 102 và sau đó mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá có trong yêu cầu tệp an toàn. Đồng thời, máy chủ quản lý 106 có thể truyền tệp liên quan đến độ an toàn động đã được mã hoá cùng với giá trị khoá mã hoá đến thiết bị máy khách 102. Trong đó, giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách 102, và do đó tệp liên quan đến độ an toàn động được mã hoá và giải mã khác nhau đối với mỗi thiết bị máy khách 102.

Tuy nhiên, khi thiết bị máy khách 102 đã truyền yêu cầu tệp an toàn là thiết bị đã đăng ký, thì máy chủ quản lý 106 có thể thu nhận giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 từ chuỗi khối 108. Máy chủ quản lý 106 có thể tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách 102, và sau đó mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được từ chuỗi khối 108. Ngoài ra, máy chủ quản lý 106 có thể truyền tệp liên quan đến độ an toàn động đã được mã hoá cùng với giá trị khoá mã hoá đến thiết bị máy khách 102. Theo đó, máy chủ quản lý 106 xác định xem thiết bị máy khách 102 đã truyền yêu cầu tệp an toàn có phải là thiết bị đã đăng ký hay không, và mã hoá tệp liên quan đến độ an toàn động bằng cách sử dụng giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách tương ứng 102, nhờ đó có thể bảo đảm thêm cho sự an toàn (tức là, độ an toàn) của ứng dụng.

Chuỗi khối 108 có thể quản lý giá trị khoá mã hoá đối với mỗi thiết bị máy khách

102. Chuỗi khối 108 có thể đăng ký thiết bị máy khách 102. Cụ thể là, khi chuỗi khối 108 thu nhận thông tin nhận dạng duy nhất của thiết bị máy khách 102 từ máy chủ quản lý 106, chuỗi khối 108 có thể xác định xem thiết bị máy khách 102 đã được đăng ký hay chưa, dựa vào thông tin nhận dạng duy nhất. Khi thiết bị máy khách 102 đang xem xét chưa được đăng ký, thì chuỗi khối 108 có thể thu nhận giá trị khoá mã hoá từ máy chủ quản lý 106 và đăng ký thiết bị máy khách 102 bằng cách so khớp giá trị khoá mã hoá và thông tin nhận dạng duy nhất của thiết bị máy khách 102.

Có nghĩa là, khi đưa ra yêu cầu tệp an toàn thứ nhất, thiết bị máy khách 102 có thể bổ sung giá trị khoá mã hoá cùng với thông tin nhận dạng duy nhất của thiết bị máy khách 102 vào yêu cầu tệp an toàn thứ nhất này. Trong đó, thiết bị máy khách 102 thu nhận và truyền giá trị khoá mã hoá chỉ khi việc kiểm tra thành công trong máy chủ kiểm tra 104, và do đó chuỗi khối 108 đăng ký thiết bị máy khách đã được kiểm tra 102.

Tuy nhiên, khi thiết bị máy khách 102 đang xem xét là thiết bị đã đăng ký, thì chuỗi khối 108 có thể tách ra giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 và truyền giá trị khoá mã hoá đã tách ra đến máy chủ quản lý 106.

Chuỗi khối 108 có thể có máy chủ giao diện lập trình ứng dụng (Application Program Interface, API) 108a và nhiều nút phân phối 108b. Máy chủ API 108a có thể tạo ra giao diện giữa máy chủ quản lý 106 và chuỗi khối 108. Máy chủ API 108a có thể thu nhận thông tin nhận dạng duy nhất của thiết bị máy khách 102 từ máy chủ quản lý 106 và xác định xem thiết bị máy khách tương ứng 102 đã được đăng ký hay chưa. Ngoài ra, máy chủ API 108a có thể lưu trữ thông tin nhận dạng duy nhất của thiết bị máy khách định trước 102 và giá trị khoá mã hoá trong nhiều nút phân phối 108b. Đồng thời, máy chủ API 108a có thể tách ra giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 từ nhiều nút phân phối 108b và truyền giá trị khoá mã hoá đến máy chủ quản lý 106.

Nhiều nút phân phối 108b có thể so khớp và lưu trữ thông tin nhận dạng duy nhất và giá trị khoá mã hoá đối với mỗi thiết bị máy khách 102. Nhiều nút phân phối 108b có thể lưu trữ thông tin nhận dạng duy nhất và giá trị khoá mã hoá đối với mỗi thiết bị máy khách 102 dựa vào công nghệ chuỗi khối. Trong trường hợp này, có thể bảo đảm tính nguyên vẹn của giá trị khoá mã hoá và có thể ngăn chặn không để cho giá trị khoá mã

hoá bị xâm nhập trái phép hoặc đánh cắp.

Theo một phương án thực hiện sáng chế, ứng dụng thiếu an toàn được phân phối cho thiết bị máy khách 120 và tệp liên quan đến độ an toàn động đã được mã hoá được truyền mỗi khi ứng dụng thiếu an toàn này được thực hiện, cho nên có thể giảm đến mức thấp nhất sự bộc lộ phần thông tin an toàn của ứng dụng được nạp vào thiết bị máy khách 102 và có thể ngăn chặn không để cho tệp liên quan đến độ an toàn của ứng dụng tương ứng bị xâm nhập trái phép hoặc đánh cắp bởi bên thứ ba có ác ý.

Ngoài ra, máy chủ kiểm tra 104 thực hiện quy trình kiểm tra ứng dụng thiếu an toàn và do đó truyền giá trị khoá mã hoá đến thiết bị máy khách 102, cho nên có thể xác nhận tính nguyên vẹn để biết ứng dụng tương ứng có bị giả mạo hoặc can thiệp hay không. Đồng thời, giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách 102, cho nên có thể cho phép quy trình mã hoá và giải mã được thực hiện khác nhau đối với mỗi thiết bị máy khách 102, nhờ đó nâng cao độ an toàn khi sử dụng ứng dụng.

Hơn nữa, ứng dụng thiếu an toàn được phân phối cho thiết bị máy khách 102, cho nên kích thước của ứng dụng được phân phối cho thiết bị máy khách 102 có thể được giảm đến mức thấp nhất, và ngay cả khi tệp liên quan đến độ an toàn động được sửa đổi hoặc cập nhật, ứng dụng này không cần phải được tải xuống lại và có thể tự động thu nhận và thực hiện tệp liên quan đến độ an toàn động đã được cập nhật ở thời điểm thực hiện ứng dụng.

Mặc dù chuỗi khối 108 được mô tả trong sáng chế dựa vào trường hợp so khớp và lưu trữ thông tin nhận dạng duy nhất và giá trị khoá mã hoá đối với mỗi thiết bị máy khách 102, nhưng phương án thực hiện sáng chế không chỉ giới hạn ở trường hợp máy chủ quản lý 106 có thể so khớp và lưu trữ thông tin nhận dạng duy nhất và giá trị khoá mã hoá đối với mỗi thiết bị máy khách 102.

Ngoài ra, mặc dù ứng dụng thiếu an toàn được mô tả trong sáng chế dưới dạng là có tệp liên quan đến độ an toàn tĩnh được nạp trên đó và không có tệp liên quan đến độ an toàn động được nạp trên đó, nhưng ứng dụng thiếu an toàn có thể không có cả hai tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động được nạp trên đó. Nói cách khác, ứng dụng thiếu an toàn có thể không có tệp liên quan đến độ an toàn nào được nạp

trên đó. Trong trường hợp này, thiết bị máy khách 102 có thể thu nhận tệp liên quan đến độ an toàn tĩnh đã được mã hoá và tệp liên quan đến độ an toàn động đã được mã hoá từ máy chủ quản lý 106 và sau đó thực hiện các tệp này sau khi giải mã các tệp.

Fig.2 là lưu đồ thể hiện quy trình kiểm tra sự giả mạo/can thiệp trong phương pháp giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế. Trong lưu đồ được thể hiện trên hình vẽ, một quy trình được thể hiện trên hình vẽ dưới dạng là được phân chia ra thành nhiều bước. Tuy nhiên, cần lưu ý rằng ít nhất một số bước trong số các bước đó có thể được thực hiện theo thứ tự khác hoặc có thể được kết hợp lại thành ít bước hơn hoặc được phân chia tiếp ra thành nhiều bước hơn. Ngoài ra, một số bước trong số các bước đó có thể được loại bỏ, hoặc một hoặc nhiều bước khác, không được thể hiện trên hình vẽ, có thể được bổ sung vào lưu đồ và được thực hiện.

Dựa vào Fig.2, thiết bị máy khách 102 tải xuống một ứng dụng thiếu an toàn (S101). Ứng dụng thiếu an toàn này là để thực hiện trực tuyến nhiệm vụ cần có độ an toàn, nhưng ứng dụng này có thể đang ở trạng thái mà ở đó nó không thể thực hiện được một cách bình thường hoặc hoàn toàn nhiệm vụ cần có độ an toàn đó vì một phần trong số các tệp liên quan đến độ an toàn bị thiếu. Theo phương án được thể hiện trên hình vẽ, thiết bị máy khách 102 có thể tải xuống ứng dụng thiếu an toàn từ thiết bị máy chủ, như máy chủ kiểm tra 104 hoặc máy chủ quản lý 106.

Sau đó, thiết bị máy khách 102 truyền yêu cầu kiểm tra liên quan đến ứng dụng thiếu an toàn đến máy chủ kiểm tra 104 (S103). Thiết bị máy khách 102 có thể truyền yêu cầu kiểm tra đến máy chủ kiểm tra 104 khi người dùng thực hiện ứng dụng thiếu an toàn. Khi ứng dụng thiếu an toàn được thực hiện trong thiết bị máy khách 102 lần đầu tiên, thiết bị máy khách 102 có thể truyền yêu cầu kiểm tra chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách 102 đến máy chủ kiểm tra 104.

Sau đó, máy chủ kiểm tra 104 thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn (S105).

Khi kết quả thực hiện ở bước S105 chỉ báo rằng thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra trùng khớp với thông tin nhận dạng đã được lưu

trữ từ trước của ứng dụng thiếu an toàn, thì máy chủ kiểm tra 104 tạo ra giá trị khoá mã hoá dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách 102 có trong yêu cầu kiểm tra (S107). Ví dụ, máy chủ kiểm tra 104 có thể tạo ra giá trị khoá mã hoá bằng cách băm thông tin nhận dạng duy nhất của thiết bị máy khách 102.

Sau đó, máy chủ kiểm tra 104 truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách 102 (S109). Thông tin liên quan đến kết quả kiểm tra chứa giá trị kết quả kiểm tra tương ứng với yêu cầu kiểm tra, thời gian kiểm tra, giá trị khoá mã hoá, và các thông tin khác. Khi kết quả thực hiện ở bước S105 chỉ báo rằng thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra không trùng khớp với thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn, thì máy chủ kiểm tra 104 có thể không đưa giá trị khoá mã hoá vào trong thông tin liên quan đến kết quả kiểm tra. Ngoài ra, máy chủ kiểm tra 104 có thể quản lý thông tin nhật ký theo yêu cầu kiểm tra của thiết bị máy khách 102.

Fig.3 là lưu đồ thể hiện quy trình thu nhận tệp liên quan đến độ an toàn động trong phương pháp giữ an toàn cho ứng dụng theo một phương án thực hiện sáng chế. Trong lưu đồ được thể hiện trên hình vẽ, một quy trình được thể hiện trên hình vẽ dưới dạng là được phân chia ra thành nhiều bước. Tuy nhiên, cần lưu ý rằng ít nhất một số bước trong số các bước đó có thể được thực hiện theo thứ tự khác hoặc có thể được kết hợp lại thành ít bước hơn hoặc được phân chia tiếp ra thành nhiều bước hơn. Ngoài ra, một số bước trong số các bước đó có thể được loại bỏ, hoặc một hoặc nhiều bước khác, không được thể hiện trên hình vẽ, có thể được bổ sung vào lưu đồ và được thực hiện.

Dựa vào Fig.3, thiết bị máy khách 102 truyền yêu cầu tệp an toàn đến máy chủ quản lý 106 khi kết quả kiểm tra của ứng dụng thiếu an toàn chỉ báo việc kiểm tra thành công (S201). Yêu cầu tệp an toàn chứa thông tin nhận dạng duy nhất của thiết bị máy khách 102, giá trị khoá mã hoá, và thông tin liên quan đến hệ điều hành của thiết bị máy khách 102. Tuy nhiên, thiết bị máy khách 102 có thể kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra của ứng dụng thiếu an toàn chỉ báo việc kiểm tra không thành công.

Sau đó, máy chủ quản lý 106 tách ra thông tin nhận dạng duy nhất của thiết bị máy khách 102 có trong yêu cầu tệp an toàn và sau đó truyền thông tin nhận dạng duy nhất đã tách ra của thiết bị máy khách 102 đến chuỗi khối 108 (S203).

Sau đó, khi có giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 (tức là, thiết bị máy khách 102 đang xem xét đã được đăng ký), thì chuỗi khối 108 tách ra giá trị khoá mã hoá và truyền giá trị khoá mã hoá này đến máy chủ quản lý 106 (S205). Mặt khác, khi không có giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 (tức là, thiết bị máy khách 102 đang xem xét chưa được đăng ký), thì chuỗi khối 108 có thể thu nhận giá trị khoá mã hoá từ máy chủ quản lý 106 và đăng ký thiết bị máy khách 102 bằng cách so khớp thông tin nhận dạng duy nhất của thiết bị máy khách 102 và giá trị khoá mã hoá.

Sau đó, máy chủ quản lý 106 tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách 102 có trong yêu cầu tệp an toàn (S207). Có nghĩa là, máy chủ quản lý 106 có thể tách ra tệp liên quan đến độ an toàn động tương ứng với loại hệ điều hành và phiên bản hệ điều hành của thiết bị máy khách 102.

Sau đó, máy chủ quản lý 106 mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được từ chuỗi khối 108 (S209), và sau đó truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá (tức là, giá trị khoá giải mã) đến thiết bị máy khách 102 (S211).

Sau đó, thiết bị máy khách 102 giải mã tệp liên quan đến độ an toàn động đã được mã hoá bằng cách sử dụng khoá giải mã thu được (S213). Ngoài ra, thiết bị máy khách 102 thực hiện tệp liên quan đến độ an toàn động bằng cách nạp tệp liên quan đến độ an toàn động đã được giải mã vào bộ nhớ và sau đó xoá tệp liên quan đến độ an toàn động (S215).

Fig.4 là sơ đồ khối để mô tả môi trường thiết bị máy tính 10 có thiết bị máy tính phù hợp được sử dụng trong các phương án làm ví dụ thực hiện sáng chế. Theo phương án được thể hiện trên hình vẽ, mỗi bộ phận trong số các bộ phận có thể có các chức năng và các khả năng khác với các chức năng và các khả năng được mô tả dưới đây và có thể có thêm các bộ phận khác ngoài các bộ phận được mô tả trong sáng chế.

Môi trường thiết bị máy tính 10 được thể hiện trên hình vẽ có thiết bị máy tính 12. Theo một phương án thực hiện sáng chế, thiết bị máy tính 12 có thể là thiết bị máy khách (ví dụ, thiết bị máy khách 102). Ngoài ra, thiết bị máy tính 12 có thể là thiết bị máy chủ

(ví dụ, máy chủ kiểm tra 104 hoặc máy chủ quản lý 106).

Thiết bị máy tính 12 có ít nhất một bộ xử lý 14, vật ghi đọc được bằng máy tính 16, và bus truyền thông 18. Bộ xử lý 14 có thể ra lệnh cho thiết bị máy tính 12 hoạt động theo phương án làm ví dụ được mô tả trên đây. Ví dụ, bộ xử lý 14 có thể thực hiện một hoặc nhiều chương trình được lưu trữ trong vật ghi đọc được bằng máy tính 16. Một hoặc nhiều chương trình này có thể chứa một hoặc nhiều lệnh thực hiện được bằng máy tính, và các lệnh thực hiện được bằng máy tính này có thể được tạo cấu hình để, khi được thực hiện bằng bộ xử lý 14, ra lệnh cho thiết bị máy tính 12 thực hiện các thao tác theo phương án làm ví dụ thực hiện sáng chế.

Vật ghi đọc được bằng máy tính 16 được tạo cấu hình để lưu trữ các lệnh thực hiện được bằng máy tính và các mã chương trình, dữ liệu chương trình và/hoặc thông tin ở các dạng phù hợp khác. Chương trình 20 được lưu trữ trong vật ghi đọc được bằng máy tính 16 có thể chứa một tập hợp gồm các lệnh có thể thực hiện được bằng bộ xử lý 14. Theo một phương án thực hiện sáng chế, vật ghi đọc được bằng máy tính 16 có thể là bộ nhớ (bộ nhớ khả biến, như bộ nhớ truy nhập ngẫu nhiên (Random Access Memory, RAM), bộ nhớ bất khả biến, hoặc dạng kết hợp của các loại bộ nhớ nêu trên), một hoặc nhiều thiết bị lưu trữ dạng đĩa từ, các thiết bị lưu trữ dạng đĩa quang, các bộ nhớ tác động nhanh, các vật ghi ở các dạng khác có khả năng truy nhập được bằng thiết bị máy tính 12 và lưu trữ thông tin cần thiết, hoặc dạng kết hợp của các loại nêu trên.

Bus truyền thông 18 kết nối các bộ phận khác nhau trong thiết bị máy tính 12 có bộ xử lý 14 và vật ghi đọc được bằng máy tính 16.

Thiết bị máy tính 12 có thể có một hoặc nhiều giao diện nhập/xuất 22 dùng cho một hoặc nhiều thiết bị nhập/xuất 24 và một hoặc nhiều giao diện truyền thông qua mạng 26. Giao diện nhập/xuất 22 và giao diện truyền thông qua mạng 26 được kết nối với bus truyền thông 18. Thiết bị nhập/xuất 24 có thể được kết nối với các bộ phận khác trong thiết bị máy tính 12 thông qua giao diện nhập/xuất 22. Thiết bị nhập/xuất 24 được thể hiện trên hình vẽ có thể là thiết bị trỏ (chuột, bàn rê chuột cảm ứng, hoặc các thiết bị tương tự khác), bàn phím, thiết bị nhập cảm ứng (bàn cảm ứng, màn hình cảm ứng, hoặc các các thiết bị tương tự khác), thiết bị nhập, như thiết bị nhập giọng nói hoặc âm thanh, các loại thiết bị cảm biến, và/hoặc thiết bị chụp ảnh, và/hoặc thiết bị xuất, như thiết bị

hiển thị, máy in, loa, và/hoặc cạc mạng. Thiết bị nhập/xuất 24 được thể hiện trên hình vẽ, là một bộ phận tạo nên thiết bị máy tính 12, có thể được bố trí ở trong thiết bị máy tính 12 hoặc có thể được tạo cấu hình dưới dạng là một thiết bị riêng biệt với thiết bị máy tính 12 và được kết nối với thiết bị máy tính 12.

Mặc dù các phương án làm ví dụ thực hiện sáng chế đã được mô tả chi tiết trên đây, nhưng người có hiểu biết trung bình về lĩnh vực kỹ thuật này cần phải hiểu rằng nhiều phương án thay đổi có thể được tìm ra mà vẫn không bị coi là vượt ra ngoài ý tưởng sáng tạo và phạm vi của sáng chế. Vì vậy, phạm vi của sáng chế được xác định dựa vào các điểm yêu cầu bảo hộ kèm theo và các phương án tương đương với các điểm yêu cầu bảo hộ, và sẽ không bị giới hạn hoặc hạn chế ở nội dung mô tả chi tiết trên đây.

YÊU CẦU BẢO HỘ

1. Hệ thống giữ an toàn cho ứng dụng bao gồm:

thiết bị máy khách được tạo cấu hình để tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động, truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn, và truyền yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động theo thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra;

máy chủ kiểm tra được tạo cấu hình để thu nhận yêu cầu kiểm tra từ thiết bị máy khách và truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách; và

máy chủ quản lý được tạo cấu hình để thu nhận yêu cầu tệp an toàn từ thiết bị máy khách và truyền tệp liên quan đến độ an toàn động đã được mã hoá đến thiết bị máy khách;

trong đó thiết bị máy khách thu nhận tệp liên quan đến độ an toàn động và giá trị khóa mã hóa từ máy chủ quản lý và giải mã tệp liên quan đến độ an toàn động đã được mã hoá dựa vào giá trị khoá mã hoá; và

tệp liên quan đến độ an toàn động chứa lệnh để kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách và nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ theo thứ tự ưu tiên được định trước khi dung lượng còn lại của bộ nhớ không đủ để nạp tệp liên quan đến độ an toàn động.

2. Hệ thống giữ an toàn cho ứng dụng theo điểm 1, trong đó yêu cầu kiểm tra chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách.

3. Hệ thống giữ an toàn cho ứng dụng theo điểm 2, trong đó máy chủ kiểm tra thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn, tạo ra giá trị khoá mã hoá dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách theo kết quả kiểm tra, và truyền thông tin liên quan đến kết quả kiểm tra chứa kết quả kiểm tra và giá trị khoá mã hoá đến thiết bị máy khách.

4. Hệ thống giữ an toàn cho ứng dụng theo điểm 3, trong đó khi có hiện tượng bất thường xảy ra, máy chủ kiểm tra tạo ra giá trị khoá mã hoá dựa vào thông tin duy nhất để quản lý trong đó kết hợp thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin quản lý giả định trước.

5. Hệ thống giữ an toàn cho ứng dụng theo điểm 4, trong đó khi tổng số lần kiểm tra không thành công theo yêu cầu kiểm tra của mỗi thiết bị máy khách trong một khoảng thời gian định trước vượt quá số lần thứ nhất định trước, thì máy chủ kiểm tra xác định rằng có hiện tượng bất thường xảy ra

6. Hệ thống giữ an toàn cho ứng dụng theo điểm 4, trong đó khi tổng số lần kiểm tra không thành công theo yêu cầu kiểm tra của thiết bị máy khách vượt quá số lần thứ hai định trước, thì máy chủ kiểm tra xác định rằng có hiện tượng bất thường xảy ra.

7. Hệ thống giữ an toàn cho ứng dụng theo điểm 3, trong đó yêu cầu tệp an toàn chứa thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

8. Hệ thống giữ an toàn cho ứng dụng theo điểm 7, trong đó máy chủ quản lý tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách, mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá, và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách.

9. Hệ thống giữ an toàn cho ứng dụng theo điểm 1, trong đó yêu cầu tệp an toàn chứa ít nhất một thông tin trong số thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

10. Hệ thống giữ an toàn cho ứng dụng theo điểm 9, trong đó hệ thống giữ an toàn cho ứng dụng này còn bao gồm chuỗi khối được tạo cấu hình để thu nhận thông tin nhận dạng duy nhất của mỗi thiết bị máy khách và giá trị khoá mã hoá từ máy chủ quản lý và so khớp và lưu trữ thông tin nhận dạng duy nhất của mỗi thiết bị máy khách và giá trị khoá mã hoá tương ứng.

11. Hệ thống giữ an toàn cho ứng dụng theo điểm 10, trong đó máy chủ quản lý truyền thông tin nhận dạng duy nhất của thiết bị máy khách có trong yêu cầu tệp an toàn đến chuỗi khối, chuỗi khối tách ra giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách và truyền giá trị khoá mã hoá đã tách ra đến máy chủ quản lý, và máy chủ quản lý tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách, mã hoá tệp liên quan đến độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được từ chuỗi khối, và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách.

12. Hệ thống giữ an toàn cho ứng dụng theo điểm 1, trong đó tệp liên quan đến độ an toàn tĩnh chứa lệnh để truyền yêu cầu kiểm tra đến máy chủ kiểm tra ở thời điểm thực hiện ứng dụng thiếu an toàn và lệnh để kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra theo thông tin liên quan đến kết quả kiểm tra chỉ báo rằng việc kiểm tra ứng dụng thiếu an toàn không thành công.

13. Phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy khách có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước:

tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động;

truyền yêu cầu kiểm tra đối với ứng dụng thiếu an toàn;

thu nhận thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra và truyền yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động theo thông tin liên quan đến kết quả kiểm tra;

thu nhận tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá tương ứng với yêu cầu tệp an toàn; và

giải mã tệp liên quan đến độ an toàn động đã được mã hoá bằng cách sử dụng giá trị khoá mã hoá;

trong đó việc giải mã bao gồm:

kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách; và

nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ theo thứ tự ưu tiên được định trước khi dung lượng còn lại của bộ nhớ không đủ để nạp tệp liên quan đến độ an toàn động.

14. Phương pháp giữ an toàn cho ứng dụng theo điểm 14, trong đó yêu cầu kiểm tra chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách.

15. Phương pháp giữ an toàn cho ứng dụng theo điểm 15, trong đó thông tin liên quan đến kết quả kiểm tra chứa kết quả kiểm tra thu được sau khi thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn và giá trị khoá mã hoá được tạo ra dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách.

16. Phương pháp giữ an toàn cho ứng dụng theo điểm 16, trong đó yêu cầu tệp an toàn chứa thông tin nhận dạng duy nhất của thiết bị máy khách, giá trị khoá mã hoá, và thông tin liên quan đến hệ điều hành của thiết bị máy khách.

17. Phương pháp giữ an toàn cho ứng dụng theo điểm 14, trong đó tệp liên quan đến độ an toàn động chứa lệnh để truyền yêu cầu kiểm tra ở thời điểm thực hiện ứng dụng thiếu an toàn và lệnh để kết thúc ứng dụng thiếu an toàn khi kết quả kiểm tra theo thông tin liên quan đến kết quả kiểm tra chỉ báo rằng việc kiểm tra ứng dụng thiếu an toàn không thành công.

18. Phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy tính có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước:

thu nhận, từ thiết bị máy khách, yêu cầu kiểm tra đối với một ứng dụng thiếu an

toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động;

thực hiện quy trình kiểm tra bằng cách so sánh thông tin nhận dạng của ứng dụng thiếu an toàn có trong yêu cầu kiểm tra và thông tin nhận dạng đã được lưu trữ từ trước của ứng dụng thiếu an toàn; và

tạo ra thông tin liên quan đến kết quả kiểm tra tương ứng với yêu cầu kiểm tra và truyền thông tin liên quan đến kết quả kiểm tra đến thiết bị máy khách;

trong đó yêu cầu kiểm tra chứa thông tin nhận dạng của ứng dụng thiếu an toàn và thông tin nhận dạng duy nhất của thiết bị máy khách và bước tạo ra thông tin liên quan đến kết quả kiểm tra bao gồm bước tạo ra giá trị khoá mã hoá dựa vào thông tin nhận dạng duy nhất của thiết bị máy khách theo kết quả kiểm tra;

trong đó thiết bị máy khách giải mã tệp liên quan đến độ an toàn động dựa vào giá trị khoá mã hoá; và

tệp liên quan đến độ an toàn động chứa lệnh để kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách và nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ theo thứ tự ưu tiên được định trước khi dung lượng còn lại của bộ nhớ không đủ để nạp tệp liên quan đến độ an toàn động.

19. Phương pháp giữ an toàn cho ứng dụng theo điểm 18, trong đó bước tạo ra giá trị khoá mã hoá bao gồm bước tạo ra giá trị khoá mã hoá bằng cách băm thông tin nhận dạng duy nhất của thiết bị máy khách khi kết quả kiểm tra chỉ báo việc kiểm tra thành công.

20. Phương pháp giữ an toàn cho ứng dụng theo điểm 18, trong đó bước tạo ra giá trị khoá mã hoá bao gồm bước xác định xem hiện tượng bất thường có xảy ra hay không dựa vào thông tin nhật ký theo yêu cầu kiểm tra của mỗi thiết bị máy khách, và khi có hiện tượng bất thường xảy ra, tạo ra giá trị khoá mã hoá dựa vào thông tin duy nhất để quản lý trong đó kết hợp thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin quản lý giả định trước.

21. Phương pháp giữ an toàn cho ứng dụng được thực hiện trong thiết bị máy tính có một hoặc nhiều bộ xử lý và bộ nhớ trong đó lưu trữ một hoặc nhiều chương trình được thực hiện bằng một hoặc nhiều bộ xử lý, phương pháp giữ an toàn cho ứng dụng này bao gồm các bước:

thu nhận, từ thiết bị máy khách để tải xuống một ứng dụng thiếu an toàn trên đó có nạp tệp liên quan đến độ an toàn tĩnh, trong số tệp liên quan đến độ an toàn tĩnh và tệp liên quan đến độ an toàn động, yêu cầu tệp an toàn đối với tệp liên quan đến độ an toàn động;

tách ra thông tin nhận dạng duy nhất của thiết bị máy khách có trong yêu cầu tệp an toàn;

truyền thông tin nhận dạng duy nhất đã tách ra của thiết bị máy khách đến chuỗi khối;

thu nhận, từ chuỗi khối, giá trị khoá mã hoá để so khớp thông tin nhận dạng duy nhất của thiết bị máy khách; và

mã hoá tệp liên quan đến độ an toàn động bằng cách sử dụng giá trị khoá mã hoá thu được và truyền tệp liên quan đến độ an toàn động đã được mã hoá và giá trị khoá mã hoá đến thiết bị máy khách;

trong đó thiết bị máy khách giải mã tệp liên quan đến độ an toàn động dựa vào giá trị khoá mã hoá; và

tệp liên quan đến độ an toàn động chứa lệnh để kiểm tra dung lượng còn lại của bộ nhớ của thiết bị máy khách và nạp một phần của tệp liên quan đến độ an toàn động vào bộ nhớ theo thứ tự ưu tiên được định trước khi dung lượng còn lại của bộ nhớ không đủ để nạp tệp liên quan đến độ an toàn động.

22. Phương pháp giữ an toàn cho ứng dụng theo điểm 21, trong đó yêu cầu tệp an toàn chứa thông tin nhận dạng duy nhất của thiết bị máy khách và thông tin liên quan đến hệ điều hành của thiết bị máy khách và bước truyền tệp liên quan đến độ an toàn động đã được mã hoá bao gồm bước tách ra tệp liên quan đến độ an toàn động tương ứng với thông tin liên quan đến hệ điều hành của thiết bị máy khách và mã hoá tệp liên quan đến

độ an toàn động đã tách ra bằng cách sử dụng giá trị khoá mã hoá thu được.

FIG. 1

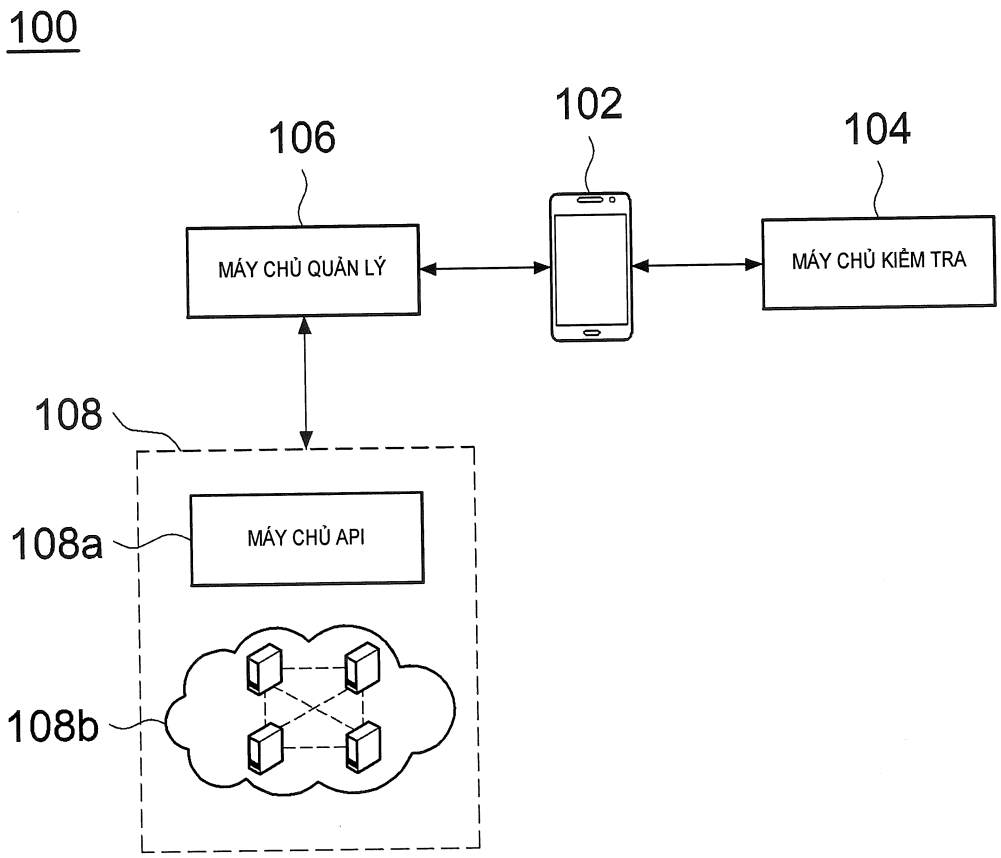

100
106
102
104
MÁY CHỦ QUẢN LÝ
MÁY CHỦ KIỂM TRA
108
108a
MÁY CHỦ API
108b

FIG. 2

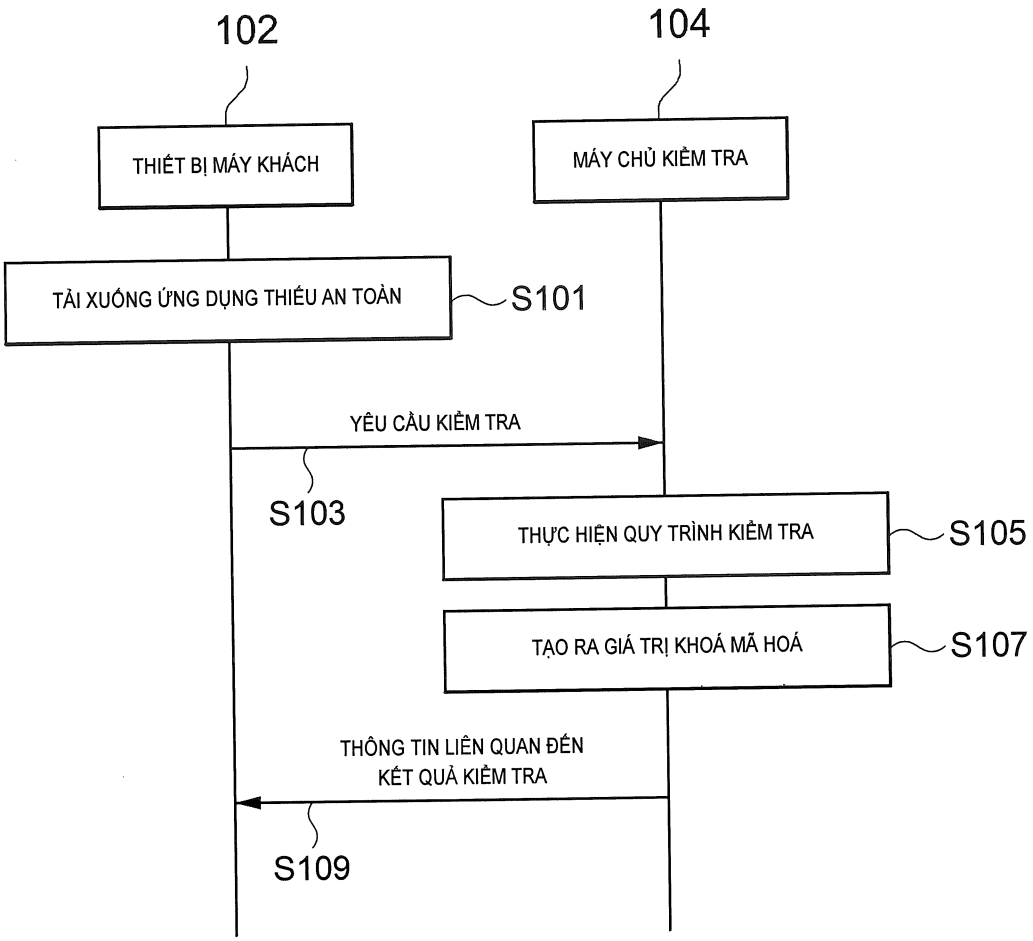

102
104
THIẾT BỊ MÁY KHÁCH
MÁY CHỦ KIỂM TRA
TẢI XUỐNG ỨNG DỤNG THIẾU AN TOÀN
S101
YÊU CẦU KIỂM TRA
S103
THỰC HIỆN QUY TRÌNH KIỂM TRA
S105
TẠO RA GIÁ TRỊ KHOÁ MÃ HOÁ
S107
THÔNG TIN LIÊN QUAN ĐẾN
KẾT QUẢ KIỂM TRA
S109

FIG. 3

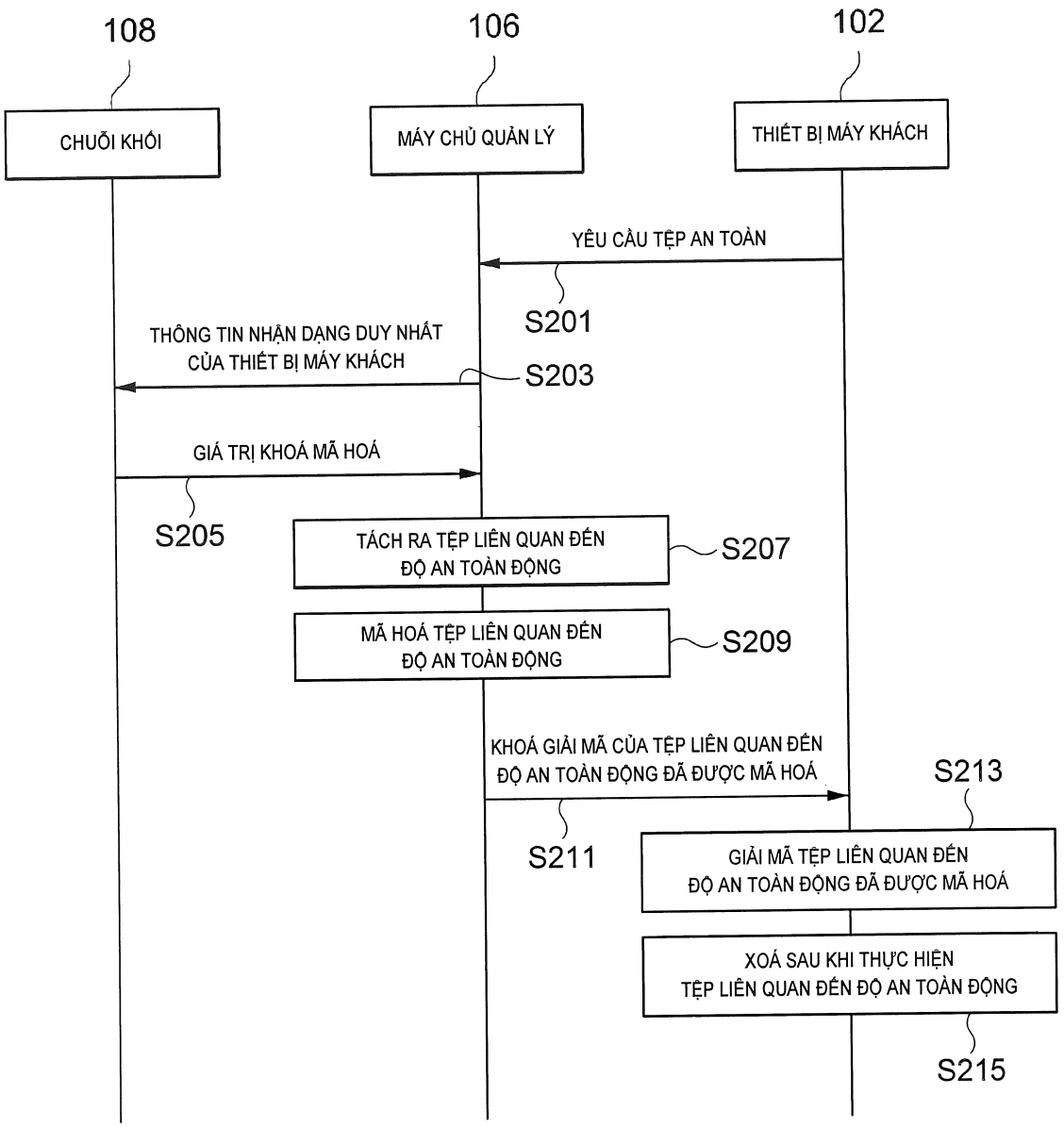
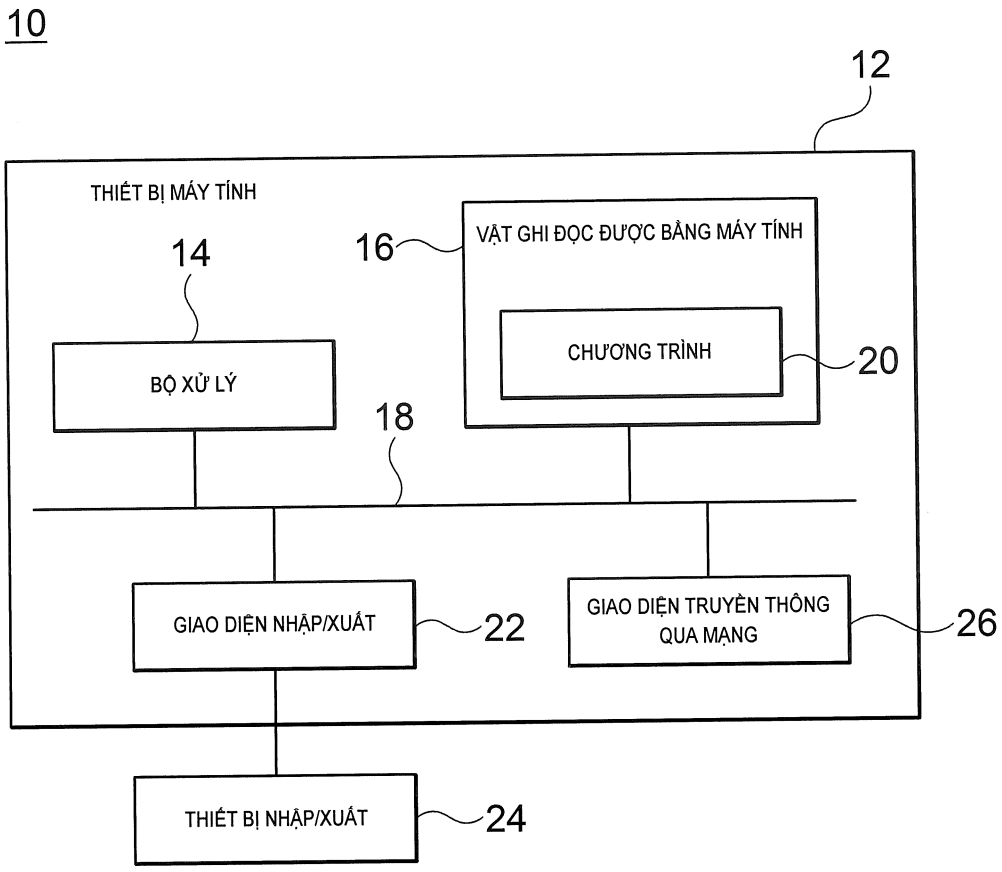

108
106
102
CHUỖI KHỐI
MÁY CHỦ QUẢN LÝ
THIẾT BỊ MÁY KHÁCH
YÊU CẦU TỆP AN TOÀN
S201
THÔNG TIN NHẬN DẠNG DUY NHẤT CỦA THIẾT BỊ MÁY KHÁCH
S203
GIÁ TRỊ KHOÁ MÃ HOÁ
S205
TÁCH RA TỆP LIÊN QUAN ĐẾN ĐỘ AN TOÀN ĐỘNG
S207
MÃ HOÁ TỆP LIÊN QUAN ĐẾN ĐỘ AN TOÀN ĐỘNG
S209
KHOÁ GIẢI MÃ CỦA TỆP LIÊN QUAN ĐẾN ĐỘ AN TOÀN ĐỘNG ĐÃ ĐƯỢC MÃ HOÁ
S211
S213
GIẢI MÃ TỆP LIÊN QUAN ĐẾN ĐỘ AN TOÀN ĐỘNG ĐÃ ĐƯỢC MÃ HOÁ
XOÁ SAU KHI THỰC HIỆN TỆP LIÊN QUAN ĐẾN ĐỘ AN TOÀN ĐỘNG
S215

FIG. 4


10
12
THIẾT BỊ MÁY TÍNH
14
16
VẬT GHI ĐỌC ĐƯỢC BẰNG MÁY TÍNH
CHƯƠNG TRÌNH
20
BỘ XỬ LÝ
18
GIAO DIỆN NHẬP/XUẤT
22
GIAO DIỆN TRUYỀN THÔNG QUA MẠNG
26
THIẾT BỊ NHẬP/XUẤT
24